Toujours un temps d'avance

Météo France

User guide

OpenAM and OpenDJ deployment

Version 2.4 Le 18/07/2016

Identifiant : –

Fichier original : `13814-02_MeteoFrance_Scripts-OpenDJ-OpenAM_Deployment-guide_v2.5.odt`

Groupe LINAGORA
80, rue Roque de Fillol
92800 PUTEAUX
FRANCE

Tél. : +33 (0)1 46 96 63 63
Fax : +33 (0)1 46 96 63 64

http://www.linagora.com/

SIRET : 431 473 669 00098

Diffusion restreinte

Diffusion : Groupe Linagora **Réf. : 13814-02**

Historique des évolutions et visas

	RÉDACTION	APPROBATION	VALIDATION
NOM	**Guy GODFROY**	**Guilhem VALENTIN**	**Guilhem VALENTIN**
FONCTION	Intégrateur système	Directeur de projets	Directeur de projets
DATE	08/01/2016	11/01/2016	11/01/2016
VISA			

Historique des évolutions

VERSION	DATE	ACTEUR CONTRIBUTEUR	OBJET DE L'ÉVOLUTION
0.1	08/01/2015	Guy Godfroy	Creation.
1.0	08/01/2015	Guilhem Valentin	Validation
2.0	02/02/2015	Guy Godfroy	Added OpenWIS configuration part
2.1	10/03/2015	Slim Cadoux	Hotfix
2.2	18/03/2015	Slim Cadoux	Modification for Security folder
2.4	18/07/2016	Guilhem Valentin	Adding configuration file generation mechanism
2.5	24/08/2016	Guilhem Valentin	Adding configuration of libIDPDiscoveryConfig.properties
2.6	23/09/2016	Claudon Michaël Goupil Yves	Tools scripts register_sp.sh

Statut du document : 60 – En application

Diffusion du document

Mention de diffusion : Groupe Linagora

NOM	ORGANISME	POUR	MÉDIA
Tous les collaborateurs du projet	LINAGORA	Information	Courriel, LinShare
Tous les collaborateurs du projet	Météo France	Action	Courriel, LinShare

Liste des contributeurs

- Guy GODFROY
- Guilhem VALENTIN
- Slim CADOUX
- Claudon Michaël
- Goupil Yves

Table des matières

1 Introduction

This document explains how to correctly setup OpenDJ and OpenAM for them to communicate each other, and a basical OpenWIS configuration, and then how to configure them in the OpenWIS point of view.

This procedure was inspired by the original OpenAM Migration manual. Everything has been automated with scripts, so graphical configuration is no longer required.

2 Communication between OpenAM and OpenDJ

The scripts of this part are in `deploy.tar.gz`.

2.1 Disclaimer

While configuring your openwis stack, you can often be stuck for many reasons. To avoid most of the bugs you need to check the following things:

- ensure your hostname is properly set in both **/etc/hosts** and **/etc/sysconfig/network**
- ensure the hostname is set with the LAN ip and not only localhost
- use the fqdn format for your hostname where is required everytime
- this host name must be resolvable by the internal dns of your LAN and / or your own server (this is also requied if you need to browse openam webUI).
- **never** declare any "localhost" in any *.properties file. **Always use their fully qualified domain name**
- ensure your firewall rules allows every connections and port you need

On a side note, if you have to reinstall the stack.

- Ensure every java processes are terminated.
- Shutdown apache-tomcat
- Use the shell command rpm -e OpenDJ* and rpm -e OpenAM*
- then erase the remaining files manually in the folder of openwis
- erase the folder openam inside apache-tomcat

2.2 Pre-requisites

Install dependencies if required:

```
yum install java-1.7.0-openjdk
yum install java-1.7.0-openjdk-devel
```

Ensure Tomcat is installed somewhere.

```
cd /home/openwis
tar zxvf apache-tomcat-7.0.68.tar.gz
```

Install OpenDJ and OpenAM:

```
sudo rpm -i OpenDJ-2.6.0-1.el6.x86_64.rpm
sudo rpm -i OpenAM-12.0.0-1.el6.x86_64.rpm
```

Security Services deployment : Refer to point 3.4 Openwis Install Guide

user openwis:

```
mkdir /home/openwis/apache-tomcat-7.0.59/webapps/openwis-securityservice

cd /home/openwis/apache-tomcat-7.0.59/webapps/openwis-securityservice

Get the artefact from OpenWIS building directory
jar xvf openwis-securityservice.war
```

Edit the configuration file: WEB-INF/classes/openwis-securityservice.properties
The following parameters need to be set:
ldap_host: set the OpenDJ host
ldap_port: keep 1389
ldap_user: keep cn=Directory Manager
ldap_password: **set the LDAP admin password configured during OpenDJ installation**

2.3 Configuration

2.3.1 Script configuration file

You have to setup your configuration in file **`deploy_config`**.

The parameters to be edited in file **`deploy_config`** are the following :

```
# OpenDJ password
OPENDJ_PASSWD=opendjpwd

# OpenAM user and password
OPENAM_USER=amAdmin
OPENAM_PASSWD=openampwd

# Install pathes
OPENAM_PATH=/home/openwis/middleware
OPENDJ_PATH=/home/openwis/OpenDJ-2.6.0
OPENAM_INSTALL_PATH=/home/openwis/openam
TOMCAT=/home/openwis/apache-tomcat-7.0.68

# URL to OpenAM and IdP
```

```
OPENAM_URL=http://hacops.lan.par.lng:8080/openam
IDPDSC_PREFIX=http://hacops.lan.par.lng:8080/idpdiscovery

# Extra OpenWis parameters
SERVER_NAME=hacops.lan.par.lng
SERVER_URL=http://hacops.lan.par.lng
SERVER_PORT=:8080
AMLDAPUSERPASSWD=linagoraagent
COOKIE_DOMAIN=.lan.par.lng
SUFFIX_OAM=dc=openam,dc=linagora,dc=local
SUFFIX_SSO=dc=linagora,dc=local

# COT name
COT=cot_openwis
```

2.3.2 Generating OpenDJ and OpenAM configuration files

Note : all configuration parameters are centralized in file **deploy_config**, so for standard deployment there is no need to change passwords and other parameters in files **setup_opendj.properties**, **setup_openam.properties** or **attrs.properties**.

The deployment script will automatically take care to generate those files. The sub-script that generates them is **deploy-configure.sh** : it can eventually be launched manually to test the generation of configuration files.

```
cd deploy-scripts
./deploy-configure.sh
```

```
Prepare setup_opendj.properties
Prepare setup_openam.properties
Prepare attrs.properties
Prepare libIDPDiscoveryConfig.properties
```

The **deploy-configure.sh** script uses the following files as templates to generate the target configuration files:

- **setup_opendj.properties.orig**
- **setup_openam.properties.orig**
- **attrs.properties.orig**
- **idp/libIDPDiscoveryConfig.properties.orig**

Those template files can refer any of the parameters defined in file **deploy_config**.

As an example, below is the file **setup_opendj.properties.orig**, with referred parameters highlighted in blue:

```
#
# Sample properties file to set up OpenDJ directory server
#
hostname                        =${SERVER_NAME}
ldapPort                        =1389
addBaseEntry                    =true
#generateSelfSignedCertificate  =false
#enableStartTLS                 =false
```

```
#ldapsPort                        =1636
jmxPort                           =2689
adminConnectorPort                =4444
rootUserDN                        =cn=Directory Manager
rootUserPassword                  =${OPENDJ_PASSWD}
baseDN                            =${SUFFIX_SSO}
```

2.4 Run the script

Then run the deployment script to deploy and configure OpenDJ and OpenAM:

```
cd deploy-scripts
./deploy.sh
```

You now have a fully configured OpenAM / OpenDJ stack.

If you need to do a server maintenance for instance, always shutdown Tomcat first, then OpenDJ.

To restart your stack properly, start OpenDJ, wait for it to be running properly, then start Tomcat.

2.5 Initialize Centre in LDAP

Refer to 3.5 OpenWIS Install Guide

When deploying a new Centre, the LDAP must be initialized.
The provided OpenWIS Archives contains a tool to perform the LDAP initialization when defining a new Centre.
Install PopulateLDAP, for example on the IdP:

```
mkdir PopulateLDAP
cd PopulateLDAP
unzip PopulateLDAP.zip
chmod a+x populateLDAP.sh
```

Configure the script populateLDAP to set the webservice location or user and group management.
Run the script:

```
./populateLDAP.sh
```

Run Populate LDAP:

- Enter 1, to create a new Centre
- Enter the Centre name (name of the deployment name: e.g. GiscMF)
- Enter the Administrator login, password, email, First name, Last name

This script creates the initial LDAP nodes for a given deployment (groups and organizational units) to allow an OpenWIS authentication.
The created groups need to be known by the portals. An automatic synchronization is done when the portal (user or admin) starts. So remind that the portal may need to be restarted (if already installed and running).

3 OpenWIS Service Provider

The scripts of this part are included in **`deploy.tar.gz`**.

3.1 Service Provider

You fisrt must generate your fedlet on your other portals before doing this step.

This script will import the remote service providers and match the attributes.

```
cd sp
./register_sp.sh
```

4 Tools

To uninstall properly, use the scripts provided in tools directory

- tomcat and OpenDJ stop

as openwis user:
./stop_opendj_tomcat.sh

- Cleaning

as root :
su -
cd /home/openwis/
./clean.sh